A multi-objective genetic algorithm for minimising network security risk and cost

Valentina Viduto, Carsten Maple, Wei Huang, Alexey Bochenkov
University of Bedfordshire
Institute for Research in Applicable Computing, (IRAC)
Luton, United Kingdom
valentina.viduto@beds.ac.uk
carsten.maple@beds.ac.uk
wei.huang@beds.ac.uk
alexey.bochenkov@beds.ac.uk

***Abstract*—Security countermeasures help ensure information security: confidentiality, integrity and availability(CIA), by mitigating possible risks associated with the security event. Due to the fact, that it is often difficult to measure such an impact quantitatively, it is also difficult to deploy appropriate security countermeasures. In this paper, we demonstrate a model of quantitative risk analysis, where an optimisation routine is developed to help a human decision maker to determine the preferred trade-off between investment cost and resulting risk. An offline optimisation routine deploys a genetic algorithm to search for the best countermeasure combination, while multiple risk factors are considered. We conduct an experimentation with real world data, taken from the PTA(Practical Threat Analysis) case study to show that our method is capable of delivering solutions for real world problem data sets. The results show that the multi-objective genetic algorithm (MOGA) approach provides high quality solutions, resulting in better knowledge for decision making.**

***Index Terms*—IT security; Genetic algorithm; Risk optimisation; Countermeasure selection problem; Decision Making;**

I. Introduction

Assuring a secure IT environment has become a major concern for decision makers, due to evolving complexity of networked systems and high number of vulnerabilities and threats. For instance, according to recent surveys undertaken in 2010, around 71% of UK organisations suffered at least one data breach in 2009 and 44% suffered between 2 and 5 breaches [1]. Globally, 88% of organisations have reported at least one data breach, which is up 3% from 2009 [2]. In fact, a high number of reported breaches is usually a good indicator that organisations have some issues with their deployed security strategies.

Risk assessment is a well understood and widely accepted ontology among decision makers, who is seeking to assure a security of corporate IT infrastructures. A number of models have been proposed to facilitate in security countermeasure selection, however, the lack of relationship among risk related factors, leads to poor and unbalanced security [3]–[5]. Often risk is expressed by measuring Annual Loss Expectancy (ALE), which is calculated by summing up the impact of outcomes in monetary units and frequency of such outcomes [6]. Further, this metric was incorporated into cost-benefit analyses to calculate Return-on-Investment (ROI) [7], [8]. Recently, risk was expressed as the product of threat occurrences and their resultant losses in US dollars, per event [9].

$$R = \sum_i E_i * L_i(C) \tag{1}$$

where R is risk in US dollars per year, i index representing threats, E_i expected number of security events of type i per year and $L_i(C)$ expected US dollar loss caused by security event given the current set of countermeasures C.

Thus, the risk assessment often involves a calculation of risk in relation to financial returns, rather than defined as risk of possible losses related to degradation of information security. Information security is commonly referred to as CIA (Confidentiality Integrity Availability) [10]. One of the first publications, where risk was associated with the impact on CIA, nevertheless only by the theoretical means, was Risk management guide for IT systems (NIST SP800-30) [11]. Hence, in this paper we demonstrate a novel approach of selecting security countermeasures with respect to both, investment cost and risk of possible degradation of CIA. Nevertheless, in this paper we provided only a basic description of the model and concentrate on a problem solving method used to support effective decision making, rather than on the model itself. A detailed analysis of the model and overall risk assessment framework can be found in [12].

The paper is organised as follows. In section II a definition of multi-objective optimisation is provided. Section III presents the mathematical model of the countermeasure selection problem, where a multi-objective function minimising cost and risk is systematically formulated. Section IV describes a developed multi-objective genetic algorithm (MOGA) as a technique to solved a problem formulated, followed by the experiment and discussion of the results of a real world case study data in Section V. Finally the conclusion is drawn in Section VI.

II. Multi-objective Optimisation

Most of the real world problems involve many objectives, often conflicting ones. Due to this conflicting nature a simple

978-1-4673-2362-8/12/$31.00 ©2012 IEEE

single objective value comparison cannot be used when a comparison of two and more feasible solutions to the problem is desired. Most multi-objective algorithms deploys a concept of dominance to perform such comparison in the multi-objective environment.

The defined optimisation problem has two objectives, without loss of generality, both to be minimised. The solution to this problem can be described in terms of a decision vector $(S_1, S_2, ...S_k)$ in the decision space. A function $f : S \rightarrow X$, $X \subseteq \mathbb{R}^k$ and $k > 1$ evaluates the quality of a specific solution by assigning an objective vector to it.

In a minimisation problem, where S and S' are two feasible solutions, and X is a decision space, i.e., $S, S' \in X$, the solution S strictly dominates or is preferred to a solution S' if each objective function value $f_p(S)$ is no greater that the corresponding objective function value $f_p(S')$, where p is an objective $1 \leq p \leq P$,and at least one objective function value is strictly less : $f_p(S) \leq f_p(S') \forall p$ and $f_p(S) < f_p(S') \exists p$.

A concept of dominance is crucial for the minimisation problem demonstrated in this paper. A solution which effectively reduces one of the objectives will adversely increase the other objective. Thus, a trade-off between these two conflicting objectives can expand the knowledge of a human decision maker on possible investments and resulting risks while selecting a set of countermeasures.

III. Formulating the problem

In general, security solutions can be classified based on the function they provide. Security solutions from one category have the unique ability to address a particular vulnerability. However, some solution from within the same category may differ from each other by technical specifications and market costs. On the whole, the classification simplifies the processes of evaluation and selection of security countermeasures.

Let each security countermeasure be represented as a single bit in the security countermeasure vector:

$$\vec{S} = \{S_l\} = \{0, 1\} \forall l, \;\; l = 1, 2, ..., k. \tag{2}$$

where S_l represents an individual security countermeasure. The value 1 indicates that this countermeasure is applied to the information system and otherwise 0.

The selection of security countermeasures is performed by first matching them to identified vulnerabilities.

Definition: *A vulnerability is a weakness or flaw in system security procedures, design or internal, management controls that can be accidentally triggered or intentionally exploited, resulting in a loss of confidentiality, integrity, availability*.

Let each vulnerability be represented as a single bit in the vulnerability vector:

$$\vec{V} = \{V_i\} = \{1, 0\} \forall i, \;\; i = 1, 2, ..., n. \tag{3}$$

where V_i represents an individual vulnerability. The value 1 indicates the presence of this vulnerability in the information systems, otherwise 0.

According to the Common Vulnerability Scoring System (CVSS), there are three impact on CIA levels: partial (P), complete (C) and none (N) [13]. The highest impact corresponds to the CCC combination, standing for complete impact on confidentiality, integrity and availability. For every CVE numbered vulnerability, such a combination of impacts can be retrieved from the National Vulnerability Database [14].

Let an impact introduced by a vulnerability be defined as I_i. Considering different PCN combinations and an impact scale taken from [11], the impact is classified as following:

$$I_i = \begin{cases} Low(10) & \text{when } CIA \in \{NNP, NPN, PNN\}; \\ Medium(50) & \text{when } CIA \in \{PPN, PNP, NPP, PPP, \\ & NNC, NCN, CNN\}; \\ High(100) & \text{when } CIA \in \{PPC, PCP, CPP, NCC, \\ & CNC, CCN, PCC, CPC, CCP, CCC\}; \end{cases}$$

Vulnerabilities, technical or nontechnical, can be identified in four ways: using automated vulnerability scanning tools, performing penetration testing, using modelling techniques to predict nontechnical system weaknesses and by assessing previous risk assessment documentation of the IT system. Once the vulnerabilities are characterized, identification of threats that can exploit them should be carried out.

Definition: *A threat is a potential cause of an unwanted event, in which a specific vulnerability is triggered or intentionally exploited.*

Humans should be considered as potentially dangerous threat sources, who through intentional or unintentional acts can carry out an attack. Intentional acts, such as an attempt to get unauthorised access,e.g., via a password guessing, or an attempt to circumvent the IT security, can be performed by disgruntled employees, malicious persons. Whether unintentional acts are initiated through negligence and errors [11]. A motivation in performing such acts should be carefully assessed as well as methods by which humans might carry out such an act. In addition, security violation reports, incident reports, history of system break-ins should be reviewed by a decision makers. Such informational sources will help to gather potential threat source data that may be a concern, where a vulnerability exists. Nevertheless, a list of threats should be tailored to individual organisations and be business oriented.

Let each threat be represented as a single bit in the threat vector:

$$\vec{T} = \{T_j\} = \{0, 1\} \forall j, \;\; j = 1, 2, ..., m. \tag{4}$$

where T_j represents an individual threat. The value 1 indicates the presence of this threat in the information systems and otherwise 0.

The likelihood L_{ji} of a threat T_j acting over a vulnerability V_i is defined as $L_{ji} = \langle T_j, V_i, \rangle$ and it can adopt one of three values: 0.1, 0.5 and 1, where the value 0.1 represents low likelihood, 0.5 - medium likelihood and 1 - high likelihood [11]. If a threat T_j has no effect on a vulnerability V_i, there is no risk and thus $L_{ji} = 0$.

Definition: *Total Initial Risk (TIR) is the sum of initial risks in an organisation, when no security countermeasures have been applied.*

TIR can be computed as follows:

$$TIR = \sum_{j=1}^{m} \sum_{i=1}^{n} L_{ij} \cdot I_i \cdot V_i, \tag{5}$$

where $TIR \in \mathbb{R}^+$, and L_{ji}, I_i, V_i are derived during the risk assessment analysis.

The value TIR indicates the total value of risk over all identified threats, vulnerabilities and resulting impacts on CIA. The purpose then is to reduce this value by selecting a set of security countermeasures.

In order to select appropriate security measures which would reduce the TIR value, a matching metric has been used, defined as z_{li}. Previously countermeasure-to-vulnerability matching idea has been proposed in [15] and later demonstrated in [16], where a matching value is assigned based on an analysis, if a countermeasure can directly address or indirectly address one or more vulnerabilities, indirectly create some vulnerability or directly create some vulnerability.

In general, z_{li} values should be assigned based on the characteristics of a countermeasure and its match with the vulnerability match. Each countermeasure-vulnerability combination z_{li} may have one of the five possible consequences:

$$z_{li} = \begin{cases} 1 & \text{if } S_l \text{ directly addresses } V_i; \\ 0.5 & \text{if } S_l \text{ indirectly addresses } V_i; \\ 0 & \text{if } S_l \text{ and } V_i \text{ do not match;} \\ -0.5 & \text{if } S_l \text{ indirectly creates } V_i; \\ -1 & \text{if } S_l \text{ directly creates } V_i. \end{cases}$$

z_{li} matching values can be derived through questionnaires and workshops with people from various parts of the organisation such as information security experts, information technology managers and staff, business asset owners and users, and senior managers. In other cases, z_{li} values can be obtained from the National Vulnerability Database(NVD) [14]. However, sources such as data breach reports, security practices and guidelines [17], [18] can be used for some countermeasure categories to deliver concise data about which vulnerabilities can be directly or indirectly created, or addressed, while a security countermeasure is implemented.

Another factor, that should be considered during a security countermeasure selection, is an investment cost. Suppose that each of the listed countermeasures has an associated cost C_l. The overall cost for a particular security countermeasure S_l is the sum of the four presented sub-costs (operational, man power, purchase and training) defined in monetary units, i.e.,

$$C_l = \sum_{n=1}^{4} C_{ln} \tag{6}$$

Definition: *Total Cost (TC)*
Given a set of k security measures, each having a cost C_l, $1 \leq l \leq k$ and considering a vector of $\vec{S} = (S_l)$, $S_l \in \{0,1\} \forall\, l,\ 1 \leq l \leq k$, the total cost TC is defined as:

$$TC(\vec{S}) = \left\{ \sum_{l=1}^{k} C_l S_l : C_l > 0,\ \forall l\ (C_l) \right\} \tag{7}$$

$$S_l = \begin{cases} 1 & \text{if a security measure } l \text{ is selected in the solution;} \\ 0 & \text{otherwise.} \end{cases}$$

The objective two, corresponding to the risk $R(\vec{S})$ is further defined as:

Definition: *Risk (R)*
Given a total initial risk TIR, a vector $\vec{S} = (S_l)$, $S_l \in \{0,1\} \forall\, l,\ 1 \leq l \leq k$ and a matching matrix z_{li} , $z_{li} = \langle S_l, V_i \rangle$, the risk R is formulated as:

$$R(\vec{S}) = \left\{ TIR - \sum_{l=1}^{k} \sum_{j=1}^{m} \sum_{i=1}^{n} L_{ji} \cdot I_i \cdot z_{li} \cdot S_l \right\} \tag{8}$$

Definition: *Multi-objective Countermeasure Selection Problem*

Given a vector of k countermeasures $\vec{S} = (S_1, S_2, ...S_k)$ defined on a finite set X of feasible solutions, and two objectives, total cost TC and risk R, consider the multi-objective combinatorial optimisation problem:

$$min\ f(\vec{S}) = [TC, R] \tag{9}$$
$$\text{subject to } \vec{S} \in X$$

IV. Description of the Multi-objective Genetic Algorithm

A Genetic Algorithm (GA) is type of metaheuristic which is used to seek for a global optimal solution in complex multi-dimensional search spaces [19]. Although GA does not guarantee to find an optimality, it has been widely deployed for solving complex multi-objective optimisation problems, in particular it is a popular technique to solve combinatorial problems [9], [20], [21] because of its efficiency in terms of convergence and diversity of solutions. GA works with the population of candidate solutions, trying to converge towards the Pareto-optimal set by removing the infeasible and dominated ones.

The proposed algorithm is shown in Algorithm 1. A search starts by initiating a population pop of randomly generated security control vectors $\vec{S}$, or chromosomes, each of them represents one potential solution to the problem. For each solution the total cost TC and risk R are calculated, following Eq. 7 and Eq. 8. A generation index gen keeps track of the number of iterations of the MOGA. Each generation proceeds as follows: an offspring population P_{off} is first created from the parent population Par_{pop} with the help of genetic operators: selection, mutation and crossover. The objective functions' values corresponding to each solution in the offspring population are also computed. The parent and offspring populations are then combined to form a new population new_{pop}. A non-dominated sorting is then applied

to rank each solution in the population. The population then is generated by selecting fittest solutions. Maintaining diversity within the population is important in order to obtain uniformly distributed solutions over the entire Pareto Front. We implement a scattered crossover function among two parents, each gene has an equal chance of coming from either parent to create children. Mutation, which occurs with a probability of 0.01, is used to provide a genetic diversity and to broaden the space, by randomly selecting and swapping two genes.

Algorithm 1: Multi-objective Genetic Algorithm

$gen = 0$;
$pop = \vec{S}$; {Initialise a population}
$Par_{pop} = P_{off}$; {Set a parent population of size P}
while $gen < gen_{max}$ **do**
  $f_c(\vec{S})$; $f_r(\vec{S})$; {Evaluate objective values of each individual}
  sort Par_{pop} {Sort the population based on the non-domination}
  Selection {Use the selection function}
  Crossover {Use the crossover operator}
  Mutation {Use the mutation function}
  $new_{pop} = Par_{pop} + ofspr_{pop}$;
  sort new_{pop}; {Sort an extended population based on non-domination}
  $new_{pop} = best_{pop}$;
  $gen = gen + 1$;
end while

The algorithm parameters are set as follows: population size = 100, number of generations = 100, crossover probability = 0.85 and mutation probability = 0.01. We ran an algorithm for five times to check for any sensitivity in solutions obtained from different initial population. Since the final solutions converged to the same optima, we excluded the presence of such sensitivity.

V. Experimental Results and Discussion

The purpose of this section is to illustrate the procedure for determining a set of countermeasures considering multiple objectives: cost and risk. The data used in the experiment has been taken from the Practical Threat Analysis (PTA) tool, which contains a database of case studies performed, real life examples and threat models, as well as published case study documents, which can be found in [22]. PTA is a calculative threat modelling methodology that is used to facilitate in assessing operational and security risks and help in defining the most appropriate risk mitigation policy. The methodology can be summarised as follows: identify system vulnerabilities, map system assets, asses the risk of the threats and define the risk mitigation plan for the analysed system architecture and configuration. The final risk mitigation plan proposed by the threat modelling methodology is composed of the countermeasures that are cost-effective against identified threats.

A. Internal Threat Case Study

A sample data has been retrieved from [23] where a case study on the performed internal threat analysis has been published and an example model provided. The final result proposed by the PTA threat model and a suite of software tools, was a risk mitigation strategy, in particular it was suggested to consider a three step mitigation strategy to reduce the system's risk in the most effective way. Notably our purpose here is only to provide an illustrative example of our procedure with the real case study data.

The first step was to define a list of vulnerabilities and match them to the threats identified within the case study (See Table I). Identified vulnerabilities posses some impact on CIA if an identified threat will exploit a particular vulnerability. The impact can be obtained from a number of e-sources by providing a CVE number. Table II is derived from the [14]. The cost as well as a list of proposed countermeasures are summarised in Table III.

TABLE I
Case Study: Data how threats match vulnerabilities

Threat sources	Threats/ Actions	Repr.	Matched vulnerability
Web User	Malicious Insider connects to internal databases/file system in order to access/modify sensitive data	T_1	V_2,V_3, V_8,V_9
	Malicious hacker connects to internal databases/file system in order to access/modify sensitive data	T_2	V_1,V_5 ,V_9
Hacker	Hacker uses HTTP requests to get access to OS resources of the Web Server	T_3	V_1,V_9
Insider	Insider may leak sensitive information over the Web	T_4	V_4,V_8,V_6,V_7
	Employees are tempted to download music/ share files/Google chat/ for personal ends	T_5	V_5,V_6

In order to calculate risk, several calculations should be carried out, following Eq. 5. Additional step that had to be made is to construct a matching matrix z_{li}, taking sample data as well as additional sources, such as [14], [17], [18].

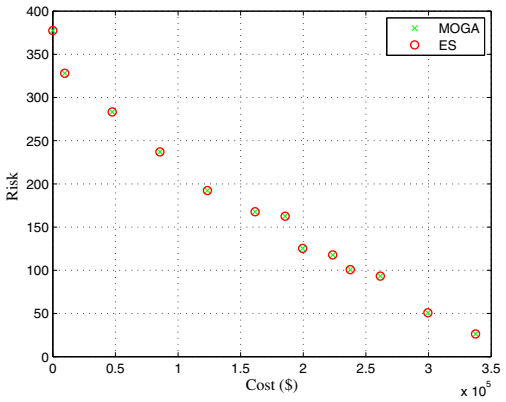

Fig. 1. Non dominated and efficient solutions

In order to ensure that an algorithm is capable of finding optimal solutions or good enough to be considered as viable, we have run an Exhaustive Search (ES). ES is considered as an only algorithm capable of finding all optimal solutions, by performing a full enumeration of solutions. Fig.1 provides

TABLE II
CASE STUDY: DATA ABOUT VULNERABILITIES AND CORRESPONDING CVE, IMPACT INFORMATION

Representation (Repr.)	Vulnerability	CVE number	Impact on CIA
V_1	Unspecified vulnerability in Microsoft IIS 6.0	2010-1256	CCC
V_2	Unauthorised data mofification	2006-0722	NPN
V_3	Insiders can execute arbitrary commands	2004-2687	CCC
V_4	Administrator password disclosure	2006-0561	CCC
V_5	Rogue protocols/tunnels	2010-4528	NNP
V_6	Traffic is not filltered properly in SNORT	2008-1804	PPP
V_7	Workstation security configuration flaws	2004-2680	PNN
V_8	FTP/HTTP file sharing	2006-3952	PPP
V_9	Multiple SQL injection vulnerabilities	2005-1503	PPP

TABLE III
CASE STUDY: DATA ABOUT COUNTERMEASURES

Repr.	Countermeasure	Mitigated Vulnerabilities	Total Cost
S1	Database login accounts should be given the minimal rights that are necessary for their functionality	V_2, V_3,$V4$,$V7$	9.500
S2	Enforce policy of downloading and deployment of latest security patches for OS, database and Web server	V_1	10.000
S3	SDLC, Enforce security code review	V_2, V_9	100.000
S4	AUP, Establish procedure and enforce for insider disclosures	V_3	75.000
S5	Alert on Web postings	V_4	38.000
S6	Alert on transfer of structured data from enterprise mgmt/design databases	V_3,V_4,V_7	76.000
S7	Monitor AUP violations	V_4,V_5,V_7	76.000
S8	Detect unauthorized non-proxied end points	V_6	76.000
S9	Monitor unusual file transfer	V_8	38.000

the result obtained by the MOGA in comparison to ES. As it can be seen, MOGA has obtained the same solutions to the ES. However, in terms of speed GA outperformed ES, in particular, it took less than a second for GA to obtain a Pareto set, whether for ES it took 15s. It should be noted, that when the size of the problem would be higher than the one analysed in this example, ES time would exponentially increase with the problem size.

Table IV summarises 13 possible sets of security countermeasures, as most effective ones to reduce threats at a corresponding cost. As it can be seen, the number of selected countermeasures within a set reaches even 6 countermeasures, depending upon the maximum budget a decision maker will consider.

TABLE IV
CASE STUDY: OBTAINED SOLUTIONS AND CORRESPONDING COUNTERMEASURES

Nr	Solution	Countermeasures selected
1	000000000	None
2	100000000	S_1
3	100000100	S_1 and S_7
4	100010000	S_1 and S_5
5	100010100	S_1,S_5 and S_7
6	100010101	S_1,S_5,S_7 and S_9
7	100011100	S_1,S_5, S_6 and S_7
8	100011101	S_1,S_5, S_6,S_7 and S_9
9	101000100	S_1, S_3 and S_7
10	101010100	S_1, S_3 and S_7
11	101010101	S_1,S_3,S_5,S_7 and S_9
12	101011100	S_1,S_3,S_5,S_6 and S_7
13	101011101	S_1,S_3,S_5,S_6,S_7 and S_9

VI. CONCLUSION

Security planning involves an ongoing risk assessment process and implementation of the most effective countermeasures which would reduce the threats and risks. As discussed, measuring risk in relation to the impact vulnerabilities introduce, is difficult. The main novelty of this paper is to demonstrate a decision support strategy when a selection of security countermeasures to be performed considering reduced risk and cost. A risk is formulated considering an impact of a security breach event (threat-to-vulnerability match) and degradation of CIA. A structured formulation of the multi-objective problem has been provided in this paper, however, the complete model can be found in [12]. To facilitate a fast and reliable search of possible countermeasure combinations, a multi-objective genetic algorithm (MOGA) has been developed and discussed. MOGA was used as an optimisation technique capable of finding optimal solutions and deriving a Pareto Set.

An example provided in the paper was based on the real data provided by the PTA. The result of the optimisation routine was a set of solutions, which upon the final decision, can be deployed to reduce the risk and meet a specified budget. Compared to full enumeration method, GA has demonstrated a great performance, in terms of speed and quality of solutions selected. Therefore, it can be considered as one of the optimisation approaches capable of dealing with a real world countermeasure selection problem.

REFERENCES

[1] C. Maple and A. Phillips, "UK Security Breach Investigations Report," 7Safe, 2010.

[2] Ponemon, "Annual Study: U.K. Enterprise Encryption Trends," Ponemon Institute, Tech. Rep., July 2010.

[3] T. Neubauer, A. Ekelhart, and S. Fenz, "Interactive selection of iso 27001 controls under multiple objectives," in *SEC*, 2008, pp. 477–492.

[4] A. Revol. (2010) Is Your IT Strategy Optimized for Risk Management. Accessed before 2011.06.13. [Online]. Available: http://www.adrien-revol.com/

[5] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security ontologies: Improving quantitative risk analysis," in *40th Annual Hawaii International Conference on System Sciences*, January 2007.

[6] K. J. Soo Hoo, "How much is enough: a risk management approach to computer security," Ph.D. dissertation, Stanford, CA, USA, 2000, AAI9986202.
[7] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *ARES*, 2006, pp. 416–423.
[8] A. Arora, D. Hall, C. A. Pinto, D. Ramsey, and R. Telang, "Measuring the risk-based value of it security solutions," *IT Professional*, vol. 6, no. 6, pp. 35–42, 2004.
[9] L. P. Rees, J. K. Deane, T. R. Rakes, and W. H. Baker, "Decision support for cybersecurity risk planning," *Decision Support Systems*, vol. 51, no. 3, pp. 493–505, 2011.
[10] T. Neubauer and C. Hartl, "On the singularity of valuating IT security investments," in *ACIS-ICIS*, 2009, pp. 549–556.
[11] *Risk Management Guide for Information Technology Systems: SP 800-30. Recommendations of the National Institute of Standards and Technology.*, NIST Std., November 2002.
[12] V. Viduto, C. Maple, W. Huang, and D. Lopez-Perez, "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem," *Accepted for publication in Decision Support Systems*, 2012.
[13] P. Mell, K. Scarfone, and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," Tech. Rep., 2007.
[14] NIST, "National vulnerability database, automating vulnerability management, security measurement and compliance cheking," http://nvd.nist.gov/home.cfm, Accessed before 1st of December 2011.
[15] R. Anderson, P. Feldman, S. Gerwehr, B. Houghton, R. Mesic, J. Pinder, J. Rothenberg, and J. Chiesa, *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*. Santa Monica, CA: RAND, 1999.
[16] M. Gupta, J. Rees, A. Chaturvedi, and J. Chi, "Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach," *Decis. Support Syst.*, vol. 41, pp. 592–603, March 2006.
[17] M.Templeman, M. Beishon, L. Malachowski, A.Wilson, T. Nash, and L. Robertson, "Information security - best practice measures for protecting your business," Department of Trade and Industry, Tech. Rep., 2005.
[18] US-CERT, "Introduction to recommended practices," http://www.us-cert.gov/control_systems/practices/, Accessed before 1st of April 2011.
[19] J. Holland, *Adaptation in natural and artificial systems*. University of Michigan Press, 1975.
[20] A. Jaszkiewicz, "Genetic local search for multi-objective combinatorial optimization," *European Journal Of Operational Research*, vol. 137, no. 1, pp. 50–71, 2002.
[21] F. Neumann, C. Witt, F. Neumann, and C. Witt, ser. Natural Computing Series. Springer Berlin Heidelberg, 2010.
[22] PTA Technologies. (2010) Practical Threat Analysis for Information Security Experts. Accessed before 2011.06.06. [Online]. Available: http://www.ptatechnologies.com/default.htm
[23] PTA. (2010) Mitigating Internal Threats with PTA. Accessed before 22nd of December 2011. [Online]. Available: http://www.ptatechnologies.com/default.htm